Installation of Shibboleth on Apache server

Prerequisites

1. **Operating System: Typically Linux-based (e.g., Ubuntu, CentOS).**
2. **Web Server: Apache installed and configured.**
3. **Dependencies:**
    - **Ensure SSL/TLS is enabled on your Apache server.**
    - **Install required libraries like libcurl, libxml2, and libxerces-c.**

Step-by-Step Installation

1. Update System

Ensure your system packages are up-to-date:

sudo apt update && sudo apt upgrade -y

2. Install Shibboleth Service Provider

- Add the Shibboleth repository for your OS:
    - **Ubuntu**:

sudo apt install software-properties-common sudo add-apt-repository ppa:shibboleth/sp sudo apt update

- **CentOS/RHEL**:

sudo yum install https://shibboleth.net/cgi-bin/sp_repo.cgi?platform=el8

- Install Shibboleth SP:

sudo apt install shibboleth-sp2-utils libapache2-mod-shib2 *# For Ubuntu* sudo yum install shibboleth *# For CentOS*

3. Enable Shibboleth Module in Apache

- Enable the Shibboleth module for Apache:

sudo a2enmod shib2 *# For Ubuntu* sudo systemctl restart httpd *# For CentOS*

- Restart Apache to load the module:

sudo systemctl restart apache2

4. Configure Shibboleth

Edit the main configuration file located at /etc/shibboleth/shibboleth2.xml.

- Set the entity ID for your service provider (SP):

<ApplicationDefaults entityID="https://your-sp-domain/shibboleth">

- Configure the IdP and SSO settings:

<SSO entityID="https://your-idp-domain/idp/shibboleth"> SAML2 </SSO>

- Ensure the <MetadataProvider> section points to your IdP's metadata URL:

<MetadataProvider type="XML" uri="https://your-idp-domain/metadata.xml" />

- Save and exit the file.

5. Secure Communication

- Ensure the server is using HTTPS. Obtain and configure an SSL certificate for your Apache server if not already done.

6. Update Apache Virtual Host

Edit your site's Apache configuration (e.g., /etc/apache2/sites-available/your-site.conf):

<VirtualHost *:443> ServerName your-sp-domain # Enable Shibboleth for specific paths <Location /secure> AuthType shibboleth ShibRequestSetting requireSession 1 Require valid-user </Location> </VirtualHost>

Enable your site and restart Apache:

sudo a2ensite your-site sudo systemctl restart apache2

7. Test Shibboleth

- Visit a protected URL (e.g., https://your-sp-domain/secure).
- Check the logs:
  - Apache logs: /var/log/apache2/error.log
  - Shibboleth logs: /var/log/shibboleth/shibd.log

Final Steps

- Exchange metadata with your Identity Provider (IdP).
- Validate SSO functionality by accessing your protected application.

Would you like help configuring the shibboleth2.xml file or setting up the IdP connection?

1. **Overview**
   1. Install prerequisites (Java, Tomcat, Apache HTTP Server).
   2. Download and install the Shibboleth IdP software.
   3. Configure the IdP (metadata, LDAP connection, etc.).
   4. Configure Apache as a reverse proxy for the IdP.

5. Secure the IdP with HTTPS.
6. Test and verify.

Step 1: Install Prerequisites

1.1 Install Java

Shibboleth IdP requires Java (OpenJDK 11 or later):

sudo apt update sudo apt install openjdk-11-jdk -y java -version *# Verify Java installation*

1.2 Install Apache Tomcat

Install and configure Tomcat to host the IdP:

sudo apt install tomcat9 tomcat9-admin tomcat9-common -y sudo systemctl enable tomcat9 sudo systemctl start tomcat9

1.3 Install Apache HTTP Server

Install Apache HTTP Server as a reverse proxy for the IdP:

sudo apt install apache2 -y

Step 2: Install Shibboleth IdP

2.1 Download Shibboleth IdP

Download the Shibboleth IdP installer:

wget https://shibboleth.net/downloads/identity-provider/latest/shibboleth-identity-provider-4.4.0.tar.gz tar -xzf shibboleth-identity-provider-4.4.0.tar.gz cd shibboleth-identity-provider-4.4.0

2.2 Run the Installer

Run the installation script and provide required details:

sudo ./install.sh

- Specify the installation directory (e.g., /opt/shibboleth-idp).
- Provide a hostname for the IdP (e.g., idp.example.com).
- Set a password for encryption keys.

Step 3: Configure Shibboleth IdP

3.1 Configure IdP Properties

Edit idp.properties located at /opt/shibboleth-idp/conf/:

sudo nano /opt/shibboleth-idp/conf/idp.properties

- Update the host:

idp.entityID=https://idp.example.com/idp/shibboleth idp.scope=example.com

- Configure LDAP (Active Directory) connection:

idp.authn.LDAP.ldapURL=ldap://ad.example.com:389
idp.authn.LDAP.baseDN=dc=example,dc=com
idp.authn.LDAP.bindDN=cn=admin,dc=example,dc=com
idp.authn.LDAP.bindDNCredential=password

3.2 Configure Metadata

Edit the metadata file /opt/shibboleth-idp/metadata/idp-metadata.xml to define your IdP entity details:

<EntityDescriptor entityID="https://idp.example.com/idp/shibboleth" xmlns="urn:oasis:names:tc:SAML:2.0:metadata"> <IDPSSODescriptor protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol"> <KeyDescriptor use="signing"> <KeyInfo> <X509Data> <X509Certificate>...</X509Certificate> </X509Data> </KeyInfo> </KeyDescriptor> <KeyDescriptor use="encryption"> <KeyInfo> <X509Data> <X509Certificate>...</X509Certificate> </X509Data> </KeyInfo> </KeyDescriptor> <SingleSignOnService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect" Location="https://idp.example.com/idp/profile/SAML2/Redirect/SSO"/> </IDPSSODescriptor> </EntityDescriptor>

Step 4: Configure Apache

4.1 Enable Required Modules

Enable the proxy and SSL modules in Apache:

sudo a2enmod proxy proxy_http ssl sudo systemctl restart apache2

4.2 Configure Reverse Proxy

Edit the Apache site configuration:

sudo nano /etc/apache2/sites-available/idp.conf

Add the following configuration:

<VirtualHost *:443> ServerName idp.example.com ProxyPreserveHost On ProxyPass /idp http://localhost:8080/idp ProxyPassReverse /idp http://localhost:8080/idp SSLEngine On SSLCertificateFile /etc/ssl/certs/idp.crt SSLCertificateKeyFile /etc/ssl/private/idp.key </VirtualHost>

Enable the site and restart Apache:

sudo a2ensite idp sudo systemctl reload apache2

Step 5: Secure with SSL

Obtain and configure an SSL certificate for your IdP domain using Let's Encrypt or another certificate authority:

sudo apt install certbot python3-certbot-apache -y sudo certbot --apache -d idp.example.com

---

Step 6: Test the IdP

12. Access the IdP endpoint: https://idp.example.com/idp.
13. Verify LDAP authentication by testing login with an AD user account.
14. Exchange metadata with a Service Provider (SP) to complete integration.

Would you like assistance with a specific part, such as LDAP or metadata configuration?

How to Integrate shibboleth ldp with Active Directory?

Integrating Shibboleth Identity Provider (IdP) with Active Directory (AD) involves configuring the IdP to use AD as an LDAP directory for user authentication and attribute resolution. Here's a step-by-step guide:

Step 1: Prerequisites

15. **Shibboleth IdP**: Installed and running on your server.
16. **Active Directory**: Access to an AD server, including:
    - **LDAP Connection**: Hostname, port (default: 389 for LDAP, 636 for LDAPS).
    - **Base DN**: e.g., dc=example,dc=com.
    - **Bind Credentials**: Username (e.g., cn=admin,dc=example,dc=com) and password.

Step 2: Configure LDAP Authentication

Edit the Shibboleth IdP authentication configuration files.

2.1 Edit idp.properties

Locate and edit the file /opt/shibboleth-idp/conf/idp.properties:

properties

Define LDAP authentication settings idp.authn.LDAP.ldapURL = ldap://ad.example.com:389 idp.authn.LDAP.useStartTLS = true idp.authn.LDAP.baseDN = dc=example,dc=com idp.authn.LDAP.bindDN = cn=admin,dc=example,dc=com idp.authn.LDAP.bindDNCredential = your-password

2.2 Edit ldap-authn-config.xml

Edit the file /opt/shibboleth-idp/conf/authn/ldap-authn-config.xml:

<bean id="shibboleth.authn.LDAP" class="net.shibboleth.idp.authn.impl.LDAPAuthenticationHandler"> <property name="ldapURL" value="%{idp.authn.LDAP.ldapURL}" /> <property name="useStartTLS" value="%{idp.authn.LDAP.useStartTLS}" /> <property name="baseDN" value="%{idp.authn.LDAP.baseDN}" /> <property name="bindDN" value="%{idp.authn.LDAP.bindDN}" /> <property name="bindDNCredential" value="%{idp.authn.LDAP.bindDNCredential}" /> </bean>

Step 3: Configure Attribute Resolution

Attribute resolution defines which user attributes (e.g., name, email) are retrieved from AD.

3.1 Edit attribute-resolver.xml

Edit the file /opt/shibboleth-idp/conf/attribute-resolver.xml:

<!-- Define the LDAP Data Connector --> <DataConnector id="myLDAP" xsi:type="LDAPDirectory" xmlns="urn:mace:shibboleth:2.0:resolver:dc"> <LDAPProperty name="ldapURL" value="ldap://ad.example.com:389"/> <LDAPProperty name="baseDN" value="dc=example,dc=com"/> <LDAPProperty name="bindDN" value="cn=admin,dc=example,dc=com"/> <LDAPProperty name="bindDNCredential" value="your-password"/> <ReturnAttributes>cn mail sAMAccountName</ReturnAttributes> </DataConnector> *<!-- Define attributes to resolve -->* <AttributeDefinition id="uid" xsi:type="Simple" xmlns="urn:mace:shibboleth:2.0:resolver:ad"> <InputDataConnector ref="myLDAP" attributeNames="sAMAccountName"/> </AttributeDefinition> <AttributeDefinition id="mail" xsi:type="Simple" xmlns="urn:mace:shibboleth:2.0:resolver:ad"> <InputDataConnector ref="myLDAP" attributeNames="mail"/> </AttributeDefinition> <AttributeDefinition id="cn" xsi:type="Simple" xmlns="urn:mace:shibboleth:2.0:resolver:ad"> <InputDataConnector ref="myLDAP" attributeNames="cn"/> </AttributeDefinition>

Step 4: Test LDAP Connection

Verify connectivity to AD using tools like ldapsearch:

ldapsearch -x -H ldap://ad.example.com -D "cn=admin,dc=example,dc=com" -w your-password -b "dc=example,dc=com"

Look for user entries and ensure the attributes (e.g., sAMAccountName, mail) are accessible.

Step 5: Update Metadata

5.1 Edit idp-metadata.xml

Ensure the IdP metadata at /opt/shibboleth-idp/metadata/idp-metadata.xml contains endpoints for the IdP:

<EntityDescriptor entityID="https://idp.example.com/idp/shibboleth" xmlns="urn:oasis:names:tc:SAML:2.0:metadata"> <IDPSSODescriptor protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol"> <SingleSignOnService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect" Location="https://idp.example.com/idp/profile/SAML2/Redirect/SSO"/> </IDPSSODescriptor> </EntityDescriptor>

Exchange this metadata with your Service Providers (SPs) for integration.

Step 6: Restart Shibboleth IdP

After making configuration changes, restart the IdP:

sudo systemctl restart tomcat9

Step 7: Test Integration

17. Access the IdP login page: https://idp.example.com/idp/profile/SAML2/Redirect/SSO.
18. Log in with an AD user.
19. Verify attribute resolution by inspecting the SAML assertion (use tools like SAML Tracer).
20. Testing the integration between Shibboleth IdP and Active Directory involves validating both authentication and attribute resolution. Here's how to thoroughly test the integration:
21.
22. **1. Test LDAP Connection**
23. Before testing Shibboleth IdP, ensure it can connect to Active Directory (AD):
24. **Command-Line LDAP Test**
25. Use ldapsearch to verify connectivity:
26. ldapsearch -x -H ldap://ad.example.com -D "cn=admin,dc=example,dc=com" -w your-password -b "dc=example,dc=com" "(sAMAccountName=username)"
27. Replace:
28. ad.example.com with your AD hostname.
29. admin,dc=example,dc=com with your bind DN.
30. username with a sample AD user.
31. Expected Output:
32. User attributes like cn, mail, sAMAccountName, etc.

33. If the test fails, troubleshoot:
34. **Host/Port**: Ensure AD is reachable and the port (389/636) is open.
35. **Credentials**: Verify bind DN and password.
36. **Base DN**: Ensure it points to the correct part of your directory tree.
37. **2. Enable Shibboleth Debug Logs**
38. To see detailed logs of LDAP authentication and attribute resolution, enable debug mode in Shibboleth:
39. **Edit** logback.xml
40. Modify /opt/shibboleth-idp/conf/logback.xml:
41. <logger name="net.shibboleth" level="DEBUG"/> <logger name="org.ldaptive" level="DEBUG"/>
42. Restart Shibboleth:
43. sudo systemctl restart tomcat9
44. Check logs at:
45. /opt/shibboleth-idp/logs/idp-process.log
46. **3. Test SSO Authentication**
47. **3.1 Access the IdP Login URL**
48. Open a browser and navigate to:
49. https://idp.example.com/idp/profile/SAML2/Redirect/SSO
50. You should see a login page.
51. **3.2 Log In with an AD User**
52. Use valid AD credentials to log in.
53. If authentication succeeds, you should be redirected to a "success" page or the Service Provider (SP).
54. **Troubleshooting Login Issues**
55. **Check** idp-process.log: Look for LDAP-related errors (e.g., incorrect credentials, base DN issues).
56. **Verify Certificates**: If using LDAPS, ensure the certificate for AD is valid and trusted by the IdP.
57.
58. **4. Test Attribute Resolution**
59. **4.1 Use a Test SP**
60. Set up a simple SAML SP or use an existing one configured with your IdP.

61. **4.2 Inspect SAML Assertion**
62. Use tools like **SAML Tracer** (a browser plugin) to capture SAML responses. Look for:
63. **Attributes**: Ensure expected attributes like sAMAccountName, mail, cn are included.
64. **Authentication Details**: Verify the user is authenticated correctly.
65. **4.3 Debug Attribute Issues**
66. Check idp-process.log for attribute resolver errors.
67. Verify attribute mappings in /opt/shibboleth-idp/conf/attribute-resolver.xml.
68.
69. **5. Test Metadata Exchange**
70. Ensure the IdP metadata is shared with SPs and vice versa:
71. **SP Metadata**: Should point to the IdP's SSO endpoints.
72. **IdP Metadata**: Ensure SP entity IDs and endpoints are correct.
73. **Example IdP Metadata Validation**
74. Access the IdP metadata URL:
75. https://idp.example.com/idp/metadata
76. Validate the XML structure.
77. Check that the entity ID matches your configuration.
78.
79. **6. Verify End-to-End SSO**
80. Log in to the SP (e.g., a test application).
81. The SP should redirect you to the IdP for authentication.
82. After logging in at the IdP, you should be redirected back to the SP and logged in.
83.
84. **7. Automate Tests**
85. For large-scale deployments, consider using testing tools like:
86. **TestShib**: A public SP for testing SAML IdP configurations (TestShib.org).
87. **SAMLtest**: A SAML assertion validation tool (samltest.id).
88.
89. **Logs to Monitor**
90. **IdP Logs**:

91. /opt/shibboleth-idp/logs/idp-process.log
92. /opt/shibboleth-idp/logs/idp-warn.log
93. **Tomcat Logs**:
94. /var/log/tomcat9/catalina.out
95. **Apache Logs**:
96. /var/log/apache2/access.log
97. /var/log/apache2/error.log